UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/606,130 | 06/24/2003 | Mithat C. Dogan | 15685P211 | 4022 |

8791 7590 05/18/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

| EXAMINER | |
|---|---|
| DINH, MINH | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | |

DATE MAILED: 05/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/606,130 | DOGAN ET AL. | |
| | Examiner | Art Unit | |
| | Minh Dinh | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) 1-37 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-37 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 24 June 2003 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-37 have been examined.

### *Claim Objections*

2. Claim 37 is objected to because of the following informalities: claim 37 is a machine-readable medium depending on claim 2, which is a method claim. It's considered that "claim 2" is a typo error. For examination purpose, claim 37 is treated as being depended upon claim 27. Appropriate correction is required.

### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-7, 10-12, 14-24, 26-32 and 35-37 are rejected under 35 U.S.C. 102(b) as being anticipated by "3G TS 33.102 V3.4.0 - 3G Security - Security Architecture" (hereinafter "3G Security").

Regarding claim 1, which is exemplary of claims 14-15 and 26, "3G Security" discloses a method comprising: establishing a master secret between a first communications device and a second communications device (fig. 16b, p. 36; Section 6.6.4.2 CK, p. 37-38); opening a connection between the first communications device

and the second communications device; generating a connection secret from the master secret; and using the connection secret for symmetric key cryptography during the connection (fig. 16b, p. 36; Section 6.6.3 Ciphering method – 6.6.4 Input Parameters to the cipher algorithm, p. 36-38).

Regarding claims 2, 16-17 and 27, "3G Security" further discloses initializing a cipher using the connection secret; and sending one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher (Section 6.6.3 Ciphering method, p. 36-37).

Regarding claims 3, 18-20 and 28, "3G Security" further discloses initializing a cipher using the connection secret; receiving one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher; and decrypting the data using the initialized cipher (Section 6.6.3 Ciphering method, p. 36-37).

Regarding claims 4 and 29, "3G Security" further discloses that generating the connection secret comprises generating an initialization vector and determining the connection secret using the master secret and the initialization vector (Section 6.6.3 Ciphering method, p. 36-37).

Regarding claims 5-6, 21-23 and 30-31, "3G Security" further discloses that the initialization vector comprises a temporal parameter, the temporal parameter comprising a hyperframe number related to the opening of the connection, the hyperframe number being functionally equivalent to an absolute frame number (Section 6.6.4.1 COUNT-C, p. 37). "3G Security" discloses that the first communication device is a wireless device

(fig. 16b, p. 36; Section 1 Scope). Inherently, the first communication device comprises an air-interface device to establish and maintain the connection.

Regarding claims 7, 24 and 32, "3G Security" further discloses that the initialization vector comprises a channel identifier, the channel identifier is an air interface parameter (Section 6.6.4.3 BEARER, p. 38).

Regarding claims 10 and 35, "3G Security" further discloses that the master secret is used for multiple connections (Section 6.4.3 Cipher key and integrity key lifetime, p. 29).

Regarding claims 11-12 and 36-37, "3G Security" further discloses that the connection comprises a communications stream and that the cipher comprises a stream cipher (fig. 16b, p. 36).

***Claim Rejections - 35 USC § 103***

5. Claims 8-9, 25 and 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over "3G Security" as applied to claims 4, 7, 29 and 32 above, and further in view of Niemi et al (2002/0035682).

Regarding claims 8, 25 and 33, "3G Security" discloses that the air interface parameters include a channel identifier (Section 6.6.4.3 BEARER, p. 38). "3G Security" does not disclose that the air interface parameters include a slot number and a frequency band identifier of a channel allocated to the connection. Niemi discloses an encryption method using air interface parameters that include a time slot number (paragraphs 0082-0083). It would have been obvious to one of ordinary skill in the art

at the time the invention was made to modify the "3G Security" method such that the air interface parameters include a time slot number, as taught by Niemi. Using parameters that change with time such as the time slot number prevents a possible eavesdropper from breaking the encryption using different messages encrypted with the same mask (paragraphs 0005-0007).

"3G Security" discloses that the method is used with a GSM network (Section 1 Scope, p. 7) which employs a combination of FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access) technologies. Accordingly, both a frequency band identifier and a time slot number are used as air interface parameters to identify a channel allocated to a connection.

Regarding claims 9 and 34, "3G Security" does not disclose that the first communications device does not sent the initialization vector to the second communications device. Niemi discloses an encryption method utilizing an initialization vector. Niemi further discloses that a first communications device does not sent the initialization vector to a second communications device (fig. 4; paragraph 0069). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the "3G Security" method such that the first communications device does not sent the initialization vector to the second communications device, as taught by Niemi, in order to save transmission bandwidth.

6. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over "3G Security" as applied to claim 12 above, and further in view of Skantze (2002/0035687).

"3G Security" does not disclose using RC4 cipher. Skantze discloses using RC4 cipher in wireless transmission (paragraph [0140]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the "3G Security" method to use RC4 cipher, as taught by Skantze. RC4 cipher is a relative fast and strong cipher.

***Conclusion***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,055,316 to Perlman et al.

U.S. Patent Application Publication No. 2002/0146127 to Wong

Menezes et al, "Handbook of Applied Cryptography"

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
5/15/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100